Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (original) An apparatus comprising:

a processor executive (PE) executable on a processor to load an operating system executive (OSE) in a secure environment, the secure environment having a fused key (FK) and associated with an isolated memory area in a platform having the processor, the OSE to manage a subset of an operating system (OS) running on the platform, the processor capable of selectively operating in a normal execution mode and, alternatively, in an isolated execution mode, the isolated memory area being accessible to the processor in the isolated execution mode;

a PE supplement comprising a PE manifest that represents the PE; and

a PE handler to verify the PE using the FK and the PE supplement.

2. (original) The apparatus of claim 1 further comprising:

a boot-up code to load the PE handler into the isolated memory area during a process of booting up the platform.

3. (original) The apparatus of claim 1 wherein the secure environment includes an OSE supplement comprising an OSE manifest that represents the OSE.

4. (original) The apparatus of claim 1 wherein the PE handler comprises:

a PE loader to load the PE into the isolated memory area; and

a verifier to verify the PE using the PE manifest.

5. (original) The apparatus of claim 1 wherein the PE handler comprises:

a PE key generator to generate a PE key using the FK;

a PE identifier logger to log a PE identifier in a storage; and

a PE entrance/exit handler to handle a PE entry and a PE exit.

6. (original) The apparatus of claim 5 wherein the PE key generator comprises:

a PE key combiner to combine the PE identifier and the FK, the combined PE identifier and FK corresponding to the PE key.

7. (original) The apparatus of claim 3 wherein the PE comprises:

an OSE loader to load the OSE and the OSE supplement into the isolated memory area;

an OSE manifest verifier to verify the OSE manifest; and

an OSE verifier to verify the OSE.

8. (original) The apparatus of claim 1 wherein the PE comprises:

an OSE key generator to generate an OSE key;

an OSE identifier logger to log an OSE identifier in a storage; and

an OSE entrance/exit handler to handle an OSE entry and an OSE exit.

9. (original) The apparatus of claim 8 wherein the OSE key generator comprises:

a binding key generator to generate a binding key (BK) using a PE key; and

an OSE key combiner to combine the OSE identifier and the BK, the combined OSE identifier and BK corresponding to the OSE key.

10. (original) The apparatus of claim 1 wherein the OSE comprises:

a module loader to load a module into the isolated memory area;

a page manager to manage paging in the isolated memory area; and

an interface handler to handle interfacing with the OS.

11. (original) The apparatus of claim 10 wherein the module comprises one or more modules selected from the group consisting of an application module, an applet module, and a support module.

12. (original) The apparatus of claim 11 wherein the OSE further comprises:

an applet key generator to generate an applet key associated with the applet module.

13. (original) The apparatus of claim 12 wherein the applet key generator comprises:

an applet key combiner to combine an OSE key with an applet identifier identifying the applet module, the combined OSE key and applet identifier corresponding to the applet key.

14. (original) The apparatus of claim 4 wherein the boot-up code comprises:

a PE locator to locate the PE and the PE supplement, the PE locator transferring the PE and the PE supplement into the PE memory at a PE address;

a PE recorder to record the PE address in a parameter block; and

an instruction invoker to execute an isolated create instruction, the isolated create instruction loading the PE handler into the isolated memory area.

15. (original) The apparatus of claim 14 wherein the isolated create instruction performs an atomic sequence, the atomic sequence being non-interruptible.

16. (original) The apparatus of claim 15 wherein the atomic sequence includes operations comprising:

reading a thread count register in a chipset to determine if the processor is the first processor in the isolated execution mode;

configuring the processor in the isolated execution mode; and

loading the PE handler into the isolated memory area.

17. (original) The apparatus of claim 15 wherein the atomic sequence of operations comprises:

verifying a loaded PE handler; and

transferring control to the loaded PE handler.

18. (original) The apparatus of claim 16 wherein the atomic sequence of operations further comprises:

reading a configuration storage in the chipset when the processor is not the first processor in the isolated execution mode; and

configuring the processor according to the configuration storage in the chipset when the processor is not the first processor in the isolated execution mode.

19. (original) The apparatus of claim 18 wherein the chipset includes at least one hub selected from the group consisting of a memory controller hub (MCH) and an input/output controller hub (ICH).

20. (original) The apparatus of claim 8 wherein the storage is in an input/output controller hub (ICH) external to the processor.

21. (currently amended) A method comprising:

loading an operating system executive (OSE) into an isolated memory area of a platform, the platform having a fused key (FK) and a processor capable of selectively operating in a normal execution mode and, alternatively, in an isolated execution mode, the OSE to manage a subset of an operating system (OS) running on the platform, the isolated memory area being accessible to the processor in the isolated execution mode, the loading of the OSE initiated by a processor executive (PE) executing on the processor; and

verifying the PE using the FK and a PE supplement having a PE manifest that represents the PE, the verification to be performed by a PE handler.

22. (original) The method of claim 21 further comprising:

loading the PE handler into the isolated memory area during a process of booting up the platform.

23. (canceled)

24. (original) The method of claim 21 wherein the PE handler performs operations comprising:

loading the PE into the isolated memory area; and

verifying the PE using the PE manifest.

25. (original) The method of claim 24 wherein the PE handler performs operations comprising:

generating a PE key using the FK;

logging a PE identifier in a storage; and

handling a PE entry and a PE exit.

26. (original) The method of claim 25 wherein generating the PE key comprises:

combining the PE identifier and the FK, the combined PE identifier and FK corresponding to the PE key.

27. (original) The method of claim 21, further comprising:

verifying the OSE after loading the OSE into the isolated memory area.

28. (original) The method of claim 21 wherein the operations performed by the PE comprise:

generating an OSE key;

logging an OSE identifier in a storage; and

handling an OSE entry and an OSE exit.

29. (original) The method of claim 28 wherein generating the OSE key comprises:

generating a binding key (BK) using the PE key; and

combining the OSE identifier and the BK, the combined OSE identifier and BK corresponding to the OSE key.

30. (original) The method of claim 21 wherein the OSE manages the subset of the OS by performing operations comprising:

loading a module into the isolated memory area;

managing paging in the isolated memory area; and

interfacing with the OS.

31. (currently amended) The method of ~~claim 29~~ claim 30 wherein the module comprises one or more modules selected from the group consisting of an application module, an applet module, and a support module.

32. (original) The method of claim 31 wherein the OSE performs further operations comprising:

generating an applet key associated with the applet module.

33. (original) The method of claim 32 wherein:

the OSE combines an OSE key with an applet identifier identifying the applet module, the combined OSE key and applet identifier corresponding to the applet key.

34. (original) The method of claim 21, further comprising:

locating the PE and the PE supplement;

transferring the PE and the PE supplement into the PE memory at a PE address during a process of booting the platform;

recording the PE address in a parameter block; and

executing an isolated create instruction during the process of booting the platform, the isolated create instruction loading the PE handler into the isolated memory area.

35. (original) The method of claim 34 wherein executing the isolated create instruction comprises performing an atomic sequence, the atomic sequence being non-interruptible.

36. (original) The method of claim 35 wherein performing the atomic sequence comprises:

reading a thread count register in a chipset to determine if the processor is the first processor in the isolated execution mode;

configuring the processor in the isolated execution mode; and

loading the PE handler into the isolated memory area.

37. (original) The method of claim 35 wherein performing the atomic sequence comprises:

verifying a loaded PE handler; and

transferring control to the loaded PE handler.

38. (original) The method of claim 36 wherein configuring the processor in the isolated execution mode comprises:

reading a configuration storage in the chipset when the processor is not the first processor in the isolated execution mode; and

configuring the processor according to the configuration storage in the chipset when the processor is not the first processor in the isolated execution mode.

39. (original) The method of claim 38 wherein the chipset includes at least one hub selected from the group consisting of a memory controller hub (MCH) and an input/output controller hub (ICH).

40. (original) The method of claim 28 wherein the storage is in an input/output controller hub (ICH) external to the processor.

41-60. (canceled)

61. (original) A system comprising:

a processor capable of selectively operating in a normal execution mode and, alternatively, in an isolated execution mode;

a memory coupled to the processor having an isolated memory area accessible to the processor in the isolated execution mode;

a processor executive (PE) executable on the processor to load an operating system executive (OSE) in a secure environment, the secure environment having a fused key (FK) and associated with the isolated memory area, the OSE to manage a subset of an operating system (OS);

a PE supplement residing in storage within the system, the PE supplement comprising a PE manifest that represents the PE; and

a PE handler to verify the PE using the FK and the PE supplement.

62. (original) The system of claim 61 further comprising:

a boot-up code to load the PE handler into the isolated memory area during a process of booting up the platform.

63. (original) The system of claim 61 wherein the secure environment includes an OSE supplement comprising an OSE manifest that represents the OSE.

64. (original) The system of claim 61 wherein the PE handler comprises:

a PE loader to load the PE into the isolated memory area; and

a verifier to verify the PE using the PE manifest.

65. (original) The system of claim 61 wherein the PE handler comprises:

a PE key generator to generate a PE key using the FK;

a PE identifier logger to log a PE identifier in a storage; and

a PE entrance/exit handler to handle a PE entry and a PE exit.

66. (original) The system of claim 65 wherein the PE key generator comprises:

a PE key combiner to combine the PE identifier and the FK, the combined PE identifier and FK corresponding to the PE key.

67. (original) The system of claim 63 wherein the PE comprises:

an OSE loader to load the OSE and the OSE supplement into the isolated memory area;

an OSE manifest verifier to verify the OSE manifest; and

an OSE verifier to verify the OSE.

68. (original) The system of claim 61 wherein the PE comprises:

an OSE key generator to generate an OSE key;

an OSE identifier logger to log an OSE identifier in a storage; and

an OSE entrance/exit handler to handle an OSE entry and an OSE exit.

69. (original) The system of claim 68 wherein the OSE key generator comprises:

a binding key generator to generate a binding key (BK) using a PE key; and

an OSE key combiner to combine the OSE identifier and the BK, the combined OSE identifier and BK corresponding to the OSE key.

70. (original) The system of claim 61 wherein the OSE comprises:

a module loader to load a module into the isolated memory area;

a page manager to manage paging in the isolated memory area; and

an interface handler to handle interfacing with the OS.

71. (original) The system of claim 70 wherein the module comprises one or more modules selected from the group consisting of an application module, an applet module, and a support module.

72. (original) The system of claim 71 wherein the OSE further comprises:

an applet key generator to generate an applet key associated with the applet module.

73. (original) The system of claim 72 wherein the applet key generator comprises:

an applet key combiner to combine an OSE key with an applet identifier identifying the applet module, the combined OSE key and applet identifier corresponding to the applet key.

74. (original) The system of claim 64 wherein the boot-up code comprises:

a PE locator to locate the PE and the PE supplement, the PE locator transferring the PE and the PE supplement into the PE memory at a PE address;

a PE recorder to record the PE address in a parameter block; and

an instruction invoker to execute an isolated create instruction, the isolated create instruction loading the PE handler into the isolated memory area.

75. (original) The system of claim 74 wherein the isolated create instruction performs an atomic sequence, the atomic sequence being non-interruptible.

76. (original) The system of claim 75 wherein the atomic sequence includes operations comprising:

reading a thread count register in a chipset to determine if the processor is the first processor in the isolated execution mode;

configuring the processor in the isolated execution mode; and

loading the PE handler into the isolated memory area.

77. (original) The system of claim 75 wherein the atomic sequence of operations comprises:

verifying a loaded PE handler; and

transferring control to the loaded PE handler.

78. (original) The system of claim 76 wherein the atomic sequence of operations further comprises:

reading a configuration storage in the chipset when the processor is not the first processor in the isolated execution mode; and

configuring the processor according to the configuration storage in the chipset when the processor is not the first processor in the isolated execution mode.

79. (original) The system of claim 78 wherein the chipset includes at least one hub selected from the group consisting of a memory controller hub (MCH) and an input/output controller hub (ICH).

80. (original) The system of claim 68 wherein the storage is in an input/output controller hub (ICH) external to the processor.

81. (currently amended) An apparatus comprising:

a machine accessible medium; and

instructions encoded in the machine accessible medium, wherein the instructions, when executed in a platform, cause the platform to perform operations comprising:

loading an operating system executive (OSE) into an isolated memory area of a platform, the platform having a fused key (FK) and a processor capable of selectively operating in a normal execution mode and, alternatively, in an isolated execution mode, the OSE to manage a subset of an operating system (OS) running on the platform, the isolated memory area being accessible to the processor in the isolated execution mode, the loading of the OSE initiated by a processor executive (PE) executing on the processor; and

verifying the PE using the FK and a PE supplement having a PE manifest that represents the PE, the verification to be performed by a PE handler.

82. (currently amended) An apparatus according to claim 81, wherein the instructions implement boot-up code that performs operations comprising:

loading the PE handler into the isolated memory area during a process of booting up the platform.

83. (original) An apparatus according to claim 81, wherein the instructions implement a PE handler that performs operations comprising:

loading the PE into the isolated memory area; and

verifying the PE using the PE manifest.

84. (original) An apparatus according to claim 81, wherein the instructions implement a PE handler that performs operations comprising:

generating a PE key using the FK;

logging a PE identifier in a storage; and

handling a PE entry and a PE exit.

85. (original) An apparatus according to claim 84, wherein the PE handler generates the PE key based at least in part on a combination of the PE identifier and the FK.

86. (original) An apparatus according to claim 81, wherein the instructions cause the platform to verify the OSE after loading the OSE into the isolated memory area.

87. (original) An apparatus according to claim 81, wherein the instructions implement the PE, and the operations performed by the PE comprise:

generating an OSE key;

logging an OSE identifier in a storage; and

handling an OSE entry and an OSE exit.

88. (original) An apparatus according to claim 87, wherein the PE stores the OSE identifier in an input/output controller hub (ICH) external to the processor.

89. (original) An apparatus according to claim 81, wherein the instructions cause the platform to perform operations comprising:

generating a binding key (BK) using a PE key; and

generating an OSE key based at least in part on a combination of an OSE identifier and the BK.

90. (original) An apparatus according to claim 81, wherein the instructions implement the OSE, and the OSE manages the subset of the OS by performing operations comprising:

loading a module into the isolated memory area;

managing paging in the isolated memory area; and

interfacing with the OS.

91. (original) An apparatus according to claim 90, wherein the module loaded by the OSE comprises one or more modules selected from the group consisting of an application module, an applet module, and a support module.

92. (original) An apparatus according to claim 91 wherein the OSE performs further operations comprising:

generating an applet key associated with the applet module.

93. (original) An apparatus according to claim 92, wherein the OSE generates the applet key based at least in part on a combination of an OSE key with an applet identifier identifying the applet module.

94. (currently amended) An apparatus according to claim 81, wherein the instructions cause the platform to perform operations comprising:

locating the PE and the PE supplement;

transferring the PE and the PE supplement into PE memory at a PE address during a process of booting the platform;

recording the PE address in a parameter block; and

executing an isolated create instruction during the process of booting the platform, the isolated create instruction loading [[a]] the PE handler into the isolated memory area.

95. (original) An apparatus according to claim 94, wherein executing the isolated create instruction comprises performing an atomic sequence, the atomic sequence being non-interruptible.

96. (original) An apparatus according to claim 95, wherein performing the atomic sequence comprises:

reading a thread count register in a chipset to determine if the processor is the first processor in the isolated execution mode;

configuring the processor in the isolated execution mode; and

loading the PE handler into the isolated memory area.

97. (original) An apparatus according to claim 95, wherein performing the atomic sequence comprises:

verifying a loaded PE handler; and

transferring control to the loaded PE handler.

98. (original) An apparatus according to claim 96, wherein configuring the processor in the isolated execution mode comprises:

reading a configuration storage in the chipset when the processor is not the first processor in the isolated execution mode; and

configuring the processor according to the configuration storage in the chipset when the processor is not the first processor in the isolated execution mode.

99. (original) An apparatus according to claim 96, wherein the chipset includes at least one hub selected from the group consisting of a memory controller hub (MCH) and an input/output controller hub (ICH).